ISO/IEC JTC 1/SC 27 N 2385

REPLACES:

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE:	Summary of National Body Comments
TITLE:	Summary of National Body comments on ISO/IEC WD 15446 (SC 27 N 2333), Information technology - Security techniques – Guide for production of Protection Profiles and Security Targets
SOURCE:	Canada, France, Germany, Ukraine, United States of America
DATE:	1999-09-29
PROJECT:	1.27.22
STATUS:	This document is being submitted for consideration at the 19th SC 27/WG 3 meeting in Columbia, MD, U.S.A., October 4 - 8, 1999.
ACTION:	**ACT**
DUE DATE:	1999-10-04
DISTRIBUTION:	P, O and L-Members W. Fumy, SC 27 Chairman M. De Soete, T. Humphreys, S. Knapskog, WG-Conveners M. Donaldson, Project Editor
MEDIUM:	Server
NO. OF PAGES:	16

Secretariat ISO/IEC JTC 1/SC 27, DIN Deutsches Institut für Normung e.V., 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: passia@ni.din.de

ATTACHMENT 1
To SC 27 N 2385

ISO/IEC WD 15446
Reference number: ISO/IEC JTC 1/SC 27 N 2333 P -member voting: Canada

Title: Comments on N 2333, Guide on the production of Protection Profiles and

Security Targets, version 0.8

Date: 1 September 1999

Source: Canada

Canada has the following comments.

Major Technical:

#	P	C	Pa	S	Comment

Minor Technical:

#	P	C	Pa	S	Comment
T1	1	1.3.1	1		The first two sentences imply a stronger relationship between a PP and a TOE than is appropriate. A PP does not state a security problem for a **given** system of product, but is more generic in nature, and may be applicable to a collection of products and systems. Also, the reference to a "PP's TOE" implies a one-to-one relationship between the PP and a TOE, which is not the case.
T2	2	1.3.1	4	3	Countermeasures are mentioned later on in this paragraph, without having been adequately introduced. The text "countermeasures in the form of" should be inserted before "IT security functions".
T3	3	1.3.3	2		The sentence: "Evaluation of the actual system against the PP and ST may be part of the acceptance process." is not entirely accurate. A system is evaluated against an ST, and claims may be made that the ST is in compliance with the PP. However, a system is not evaluated against a PP. Perhaps it would be best to say that part of the acceptance process might be to submit a ST that conforms to the PP, and then have the TOE successfully evaluated against the ST.
T4	9	2.4	1		Item a) should be retitled "Executive Decision Makers/Procurers", since that is the audience that this bullet point is trying to address. The term "Consumers" is too broad in scope.
T5	10	2.4	1		Items d) and e) should be combined together, since PP/ST evaluators and TOE evaluators are not really different audiences for these purposes.
T6	11	2.6			This section seems to be placed too early in this document. At this point, we haven't even gone through the process of creating a single PP just yet. The process of creating a PP should be explained in detail before discussing the concept of a PP family.

ISO/IEC WD 15446
Reference number: ISO/IEC JTC 1/SC 27 N 2333 P -member voting: Canada

Editorial:

#	P	C	Pa	S	Comment
X1					There is a need to standardise on the exact terminology used in this document, and the terminology from the CC should be used to whatever extent possible. Some suggested terms are provided below, but the most important thing is that whatever terms are used, they are used consistently the same throughout. "Security Environment" should be used throughout, rather than "Environment" or "TOE Security Environment". When distinguishing between IT and non-IT aspects of the security environment, the terms "IT Environment" and "Non-IT Environment" should be used. "Security Policy" should be used in place of just "Policy". Thus, "Organisational Policies" and "TOE Policies" should be replaced with "Organisational Security Policies" and "TOE Security Policies" respectively. "Security Objectives" should always be used in place of just "Objectives". To refer specifically to those security objectives that apply to the TOE, the term "TOE Security Objectives" should be used. To refer specifically to those security objectives that apply to the security environment, one of the following terms "Security objectives for the environment", "Security objectives for the IT environment", or "Security objectives for the non-IT environment" should be used, as applicable. "IT Security Requirements" should be the generic term that is always used to encompass all functional and assurance requirements that apply to the TOE and the IT Environment. To refer specifically to those security requirements that apply to the TOE, the term "TOE security requirements" should be used. To refer to those security requirements that apply to the IT environment, the term "Security requirements for the IT environment" should be used.
X2	1	1.2	1	2	Insert "an" before "authority"
X3	1	1.3.1	1		In bullet c), change "Objectives" to "Security objectives that"
X4	7	2.2	3		In bullet b), change "components (domains)" to "domains". This will ensure that "component" is not used in an unnecessary fashion.
X5	7	2.2	4		Insert the text: "to that effect" at the end of the paragraph, after "appropriate statement".
X6	6,7	2.2	2-4		These paragraphs would be better placed at the end of section 2.2, so that the main focus remains on the contents of each of the PP sections. When doing this, the word "however" should be removed from paragraph 2.
X7	8	2.3	2		This paragraph should be moved to the end of section 2.3, so that the main focus remains on the contents of each of the ST sections.
X8	10	2.4	3		Delete first instance of "TOE", change "description" to "Description", and insert "TOE Security" before "Environment".
X9	10	2.4	4		Change first instance of "TOE" to "IT Security"

ATTACHMENT 1
To SC 27 N 2385

ISO/IEC WD 15446
Reference number: ISO/IEC JTC 1/SC 27 N 2333 P -member voting: Canada

X10	11	2.7	2	3	Organisational security policies should be included in this sentence, and “IT” should be inserted before “security requirements ”

ATTACHMENT 2
To SC 27 N 2385

AFNOR 29 September 1999

French comments on document SC 27 N2333 « Guide for production of PPs and STs, Version 0.8 »

N°	Chapter	Page	Remarks
1	Global		There are too many pages in this document. A PP has generally about 50 to 60 pages. This guide contains 148 pages. How can this guide help a PP writer ? Why should a PP writer read this guide instead of taking another PP as model ? Some things are repeated many times. For example, for the definition of threats, there are : - pages 19 to 23 : definition of what is a threat - page 71 : advices in how to write a threat - pages 75 to 76 : examples of threats This is too much.
2	2.4	10	It's noted that "PP objectives may be summarised in preceding sections" (i.e. in the TOE Introduction, TOE Description and Environment sections). In the CC, the objectives are described only in the Security Objectives section, not before. We propose to change « PP objectives » by « PP intends ».
3	3.2.1	13	PP Overview : what is an "Executive Summary" ?
4	6.2.1	33	first b) : if these additional SFRs are necessary to ensure that the security objectives are achieved, there should be in the "principal SFRs".
5	6.2.4	38	« Principal SFR » and « Supporting SFR » are not defined in the CC. So, we propose to delete these two notions.
6	6.2.6	40	FMT_MSA.3.1 example : in this example, a part of the requirement which is not an operation has been changed. I think a PP author has no right to modify the text of the requirements. He only can complete operations. If he wants to give details or to adapt a part of the requirement, he can add a refinement.
7	figure 5	47	In this document, the SOF claims appears only in ST at the level of the TSF. In the CC, this is although a request for the TOE security requirement statement (APE_REQ.1.10C and ASE_REQ1.9C).
8	8.3.1	53	The item a) ("the purpose of each security objective in respondind to the identified security needs") should be done in the security objectives rationale, not in the security requirements rationale.
9	8.3.1	53	The item c) ("how dependencies are accommodated") should be done in the paragraph "How to show the security requirements are mutually supportive".
10	8.3.4	56	FPT_RVM.1 : this component is in the part 2 of the CC, but it should be in the part 3 as it doesn't provide functionnal requirement but assurance requirement. So, it should not be mentionned in this guide.
11	9.3.5	60	The PP author should also have to show that the additional security requirements are "consistent" with the other security requirements.

N°	Chapter	Page	Remarks
12	10.2.4	63	b) : in the composite TOE, there can be more functionnal requirements than in the individual components. In this case, the ST author has to explain why he has chosen these requirements. This comment is also valid for all the section 10.2
13	10.2.6	65	d) : last sentence : how can this be done ("the composite TOE PP rationale should discuss any interrelationships or dependencies between different components") ?
14	Annex A	70	This annex is not really necessary as it's a re-wording of the beginning of the document.
15	A.8	74	In the ST rationale, there should be the TSS rationale too, which doesn't appear here.
16	Annex C	94	Why is this annex in the document ? There is no reason. The examples of threats in objectives provided in Annex C are the same than the one in Annex B. There is no reason to include a glossary of cryptographic terms in this guidance.
17	Annex D, E, F	124	There is today a lot of PPs that have been evaluated in the world. There is no interest to put in this document an example which has been completely created for the guide. Moreover, the PP are not complete. So, we propose to delete Annexes D,E and F.
18	Annex F	144	It is not authorized to change the title of the security requirements from Part 2.

ATTACHMENT 2
To SC 27 N 2385

AFNOR 29 September 1999

Additonal comments from France on ISO/IEC WD 15446 (SC 27 N 2333):

1) Delete comment N° 4

2) Add the following comment :
Chapte 6.2.4 Page 38:
It would be interesting to give more details for the class FMT. In the part 2 of CC, when there are management activities, it is difficult to know in what requirement of the FMT class these management activities have to be included.

3) Remark N° 7 : replace "TSF" by "TSS"

4) Remark N°12 : delete "b)" at the beginning of the remark.

5) Remark N°16 : replace "threats in objectives" by "threats and objectives".

Sylvie Arbouy
AFNOR/DTIC
France

ATTACHMENT 3
to SC 27 N 2385

German NB Comments on Project 1.27.22 (WD 15446) "Guide for production of Protection Profiles and Security Targets" (ISO/IEC JTC 1 SC 27 N 2333)

The German NB thanks the editor for providing a new WD 15446) (SC27 N2333) but regrets to note that after the many changes made the document is not very mature again, especially regarding internal consistency. The German NB also provides the following comments:

General comments:

Please make clear that STs can exist independently from PPs, confer e.g. detailed comment No. 4. Therefore please check all passages, where PPs and STs are mentioned together.

Please replace the term "non-IT security requirements" by the term "security requirements for the non-IT environment" as used in ISO/IEC 15408-1, Annex B, Subclause B.2.6 b).

In the worked examples (Annex D - Annex F) please note, which PPs and STs were the basis of the experiences and give the respective references.

The worked examples should contain at least one example with explictly stated security requirements not contained in ISO/IEC 15408.

Please replace references to "ISO 15408" by references to "ISO/IEC 15408".

Referencing to pages, as e.g. in chapter 2.6 and 3.2.1 will probably lead to problems, when the layout of the document is changed.

Detailed comments:

1) Subclause 1.3.1 "Purpose of a PP", item a):

Please make clear that the "statement of need" is not a seperate chapter in a PP but part of the PP overview.

2) Subclause 1.3.1 "Purpose of a PP", paragraph 7:

The first sentence leads to questions: Can "Requirements" solve problems? The sentence also gives the impression that the statement of need is part of the environmental description and the security objectives. In the paragraphs just before it is called out as a seperate item besides these two other items.

3) Subclause 1.3.1 "Purpose of a PP", paragraph 9:

The differences between "vulnerabilities" and "threats" and their relationship to countermeasures remain unclear. Please make clear that the threats come from outside te TOE while vulnerabilities are "properties" of the TOE.

4) Subclause 1.3.2 "Purpose of an ST", paragraph 11:

The passage "detailing how the PP's requirements are realised" leads to the misunderstanding that every ST refers to a PP. Please delete the passage.

5) Subclause 1.3.3 "Usage of the PP and ST", paragraph 13:

Please make clear that PPs are not to be written for specific IT systems. Please confer the definitions for products, systems and PPs in ISO/IEC 15408-1 and additionally the background information about products and systems in section 4.1.2 of ISO/IEC 15408-1.

6) Subclause 2.2 "Usage of the PP and ST", items a) to c):

Please make clear that the section numbers refer to those in table 1.

7) Subclause 2.4 , paragraph 53-55

Relating certain sections in a PP/ST to certain groups in the audience shouldn't be made so strict, as e.g. consumers also need access to the TOE requirements, and developers should consider the information about the TOE Security Environment.

8) Subclause 2.4 , paragraph 54

Please replace "TOE Introduction" by "PP/ST Intoduction" and replace "Environment" by "TOE Security Environment".

9) Subclause 2.6 , paragraph 60, sentence 2

Please add at the end "(and with a different TOE Security Environment and different security objectives)".

10) Subclause 3.2.1, paragraph 79, sentence 2

Add "they" before "optionally".

11) Clause 10:

Please rename the clause to "PPs and STs for Composite and Component TOEs"

12) Annex F Subclause F.3.1

It remains unclear, why the SFRs CERTGEN and DIGITSIG that are refinements of the ISO/IEC 15408 components, got a new name.

ATTACHMENT 4
to SC 27 N 2385

Comments of Ukraine on ISO/IEC WD 15446.

Page IV, 8.2
“in a” instead of “In A”

Page 5, [GMITS]
Part 4: “Selectionn of Safeguards” instead of “Baseline approach”
Part 5: “ Safeguards for external connection” instead of “Application of IT Security services and mechanisms”

(63), 1 line
[15408-2] instead of [15408-1]

(66), 1 line
“a product” instead of “an product”

(76), 2 line
“If” instead of “It”

(182)
“requirements” instead of “requirement”

(217)
“FMT” instead of “FIA”

US Comments on SC27 N2333, Guide for the Production of Protection Profiles and Security Targets, 1999-07 (WD 15446)

1. Page 1, clause 1.3.1, paragraph 6: The second sentence is unnecessary and should be deleted.
2. Page 1, clause 1.3.1, item 6c: objectives do not refine the environment, they scope the evaluation based on the stated environment. Rewrite the phrase accordingly.
3. Pages 1–2, clause 1.3.1, itemized list: the sentence structures in the list should be made parallel: make each phrase an extension of the leading sentence, not a sentence in itself. For instance change 'refine' in item c to 'refining'
4. Page 2, clause 1.3.1, paragraphs 7,8: these should be added to the list above as they are part of the PP (making parallel structure)
5. Page 2, clause 1.3.1, paragraph 7, second sentence): the security functional requirements (SFRs) do not place requirements on the users of the TOE, they are the requirements that the TOE must meet. There may be requirements on the environment, but this would be on the IT environment. Rewrite accordingly.
6. Page 2, clause 1.3.1, paragraph 7, last sentence: the term 'reliably' and be misinterpreted and isn't how we normally describe assurance. Change the sentence to read 'The assurance requirements explain the degree of confidence expected in the security functions of the TOE.'
7. Page 2, clause 1.3.1, paragraphs 9,10: remove these paragraphs as this is too much detail for this general purpose statement.
8. Page 2, clause 1.3.2, parqagraph 11, first sentence: language is too informal, change 'is like' to 'is similar to'.
9. Page 2, clause 1.3.3, paragraph 12: the use of 'product and system' opens the problems of defining these (which is why these terms were avoided in the standard). A PP or ST may apply to subsystems as well, or to a set of products grouped together but not in a specific environment (which is the definition of system in the standard.) The current sentence should be rewritten to allow all these combinations. In addition, the e.g. phrase seems to imply that all the items listed are systems and not products.
10. Page 2, clause 1.3.3, paragraph 13: the first sentence is awkward. Suggest 'A PP may also define the security needs to be satisfied by a specific system.' Delete the rest of that sentence.
11. Page 2- 3, clause 1.3.3, second sentence in paragraph 13: The second sentence should then be simplified. It currently is unclear whether the set of parties lists are all called the developer, or just the last one in the list.
12. Page 3, clause 1.3.3, paragraph 13, phrase starting 'thus for example': make this phrase a parenthetical: 'i.e., the ST written in response to an RFP (Request for Proposal) that references the PP). In addition, one of the terms should be chosen (RFP or ITT) and then the glossary could explain that it is sometimes referred to as the other.
13. Page 3, clause 1.3.3, paragraph 13, last 2 sentences: this implies that non-security requirements are part of the PP, which is not true. Non- security system requirements are not part of the evaluation, as defined in the standard. However, it is an important explain that security requirements are just part of the picture and that they must be integrated into the actual functions of the system. They are part of the trade off of performance, cost, and time to field. Either delete these two sentences or include a more complete discussion in its own paragraph, or perhaps section.
14. Page 3, clause 1.3.3, paragraph 14: combine this sentence with the above paragraph. It is an incomplete thought standing alone.
15. Page 3, clause 1.4, paragraph 18: the standard clearly states that no structure is required, and therefore cannot be implied. This guidance document should not prefer a structure as well. However, it can be said that the guidance follows the order of the PP contents as outlined in Figures B.1 and C.1 in 15408-1.
16. Page 6, clause 2.2, paragraph 31,second sentence: see comment 15 above. This structure is neither necessary nor preferred. In particular, experience has shown that rationale is most helpful when incorporated into the sections referred (rationale for objectives inline with the objectives). In addition,

the application notes are not called for in the standard, and any such notes should be in-line as well. They would likely be part of the rationale statement. His applies to the first paragraph of clause 2.3 as well.

17. Page 7, clause 2.2, paragraph 37: the TOE environment does not state the ‘security needs’ of the TOE, it states the context in which the TOE resides. ‘Security needs’ sounds like requirements and this is inappropriate. Rewrite this sentence to reflect the purpose of the security environment. This applies to the same material in clause 2.3 as well.
18. Page 9-10, clause 2.4, list: this list omits one of the most important audience uses: evaluators need to know the requirements they are measuring against. Add this to the list.
19. Page 10, clause 2.4, paragraph 55: The TSS is written for evaluators more than developers. In fact the TSS is written by the developer to say what they will implement to meet the requirements. It is therefore written for both consumers and evaluators.
20. Page 10, clause 2.4, paragraph 56: This is a confusing paragraph. A PP is a public document, and therefore the requirements therein would be available. The requirements for user documentation are clear in AGD (and other places). The purpose of the paragraph is unclear so the best thing would be to remove it.
21. Page 11, clause 2.5, list item 59b: The PP claims are not part of the rationale, but their own section/requirements. Remove ‘part of the Rationale’
22. Page 11, clause 2.6: This section is out of place and incomplete. The concept of families has always been by product/system type (and O/S family and a Firewall family). Remove this section to the end of the chapter (or to a section at the end of the document) or remove it altogether. If it is included, it needs to be further developed.
23. Page 11, clause 2.7, paragraph 63,first sentence: remove ‘which is reflected in this guide’ as unnecessary
24. Page 11, clause 2.7, paragraph 64, third sentence: replace ‘will’ with ‘may’
25. Page 13, clause 3.2.1, PP identification: This section forces repetition with later sections. It should suggest no more than the requirements dictate. The identification section is labeling information only: delete current material and rewrite to reflect 15408-1, clause B.2.2a)
26. Page 13, clause 3.2.1, PP Overview: delete paragraph 74. A separate executive summary is not required, nor preferred. The PP Overview should be no longer than an executive summary would be. It is meant to be an abstract on a registry and therefore should not be more than one or two paragraphs.
27. Page 13-14, clause 3.2.1, Related PPs: remove this section as unnecessary. In addition, it is not the PP writer’s responsibility to say how their PP relates to others. This would be a never-ending task of reviewing every time a new PP was created or updated. This may be an interesting registration detail, but that is outside this document.
28. Page 14, clause 3.2.1, PP Organisation: It is common for a document to provide a section on how it is organised, whether a preferred structure is used or not. This can be stated plainly. In addition, all the material (paras 77 – 85) on the details of each section of the PP/ST should be removed as that is (or should be) covered in those related sections.
29. Page 15, clause 3.2.2: This section forces repetition with other sections. This section should be rewritten to only reflect 15408-1, section B.2.3. In particular, items d and e in the list should be removed, along with the corresponding explanatory paragraphs (89 and 90).
30. Page 16, clause 3.2.3: application notes are not a section but would rather be integrated into text throughout the PP/ST. This should be stated as the norm. Remove paragraph 94 as the reference to hyperlinks is inappropriate (and only first mentioned there.)
31. Page 16, clause 3.3.2: The TOE description is not described differently for the ST than the PP (in 15408-1). The description therefore does not need a detailed physical and logical definition.
32. Page 17, clause 4.1, paragraph 100: delete last phase after ‘defined’ as superfluous.
33. Page 17, clause 4.1, paragraph 101: This sentence is awkward. Reword as ‘ As a general principle, statements or requirements should state what is to be accomplished without discussing how it is to be

accomplished.' The second sentence is false: the requirements do not mandate how, this is done in the specification. Requirements should always minimise dictating implementation details.

34. Page 18, clause 4.2, paragraph 104a: remove 'assumptions about' as this is in the leading phrase

35. Page 18, clause 4.2, paragraph 104b: change 'physical' to 'environmental' as it is more general (could be other than physical protection)

36. Page 19, clause 4.3, paragraph 111: add that it is encouraged to extrapolate the threats being addressed by the OSPs in order for maximum reuse of the PP, as well as for a more thorough understanding of the security problem being addressed.

37. Page 19, clause 4.3, paragraph 113: per 15408-1, clause 4.3.1, threats are always considered in terms of threat agent, method of attack, vulnerabilities, and assets. This paragraph should be rewritten to reflect this definition.

38. Page 21, clause 4.3.1, paragraph 123: This paragraph is confusing. The environment is determined and expressed in terms of assumptions and requirements in the PP/ST. It is true that 15408 does not address determining that a specific environment meets the stated assumptions. However, a vulnerability analysis of the TOE is done in light of those assumptions. Please reword this paragraph to be clearer.

39. Page 21, clause 4.3.2: this material is redundant with clause 4.3.1. Either delete the section or merge the two together.

40. Page 22, clause 4.3.2, paragraph 132, last sentence: This makes no sense – certainly a more descriptive label cannot be less explanative than a simple number. Remove this sentence.

41. Page 22, clause 4.3.2, paragraph 133, last sentence: insert 'be' between 'can' and 'taken'

42. Page 26, clause 5.1: In general, clause 5 fails to stress the fact that the security objectives outline what a TOE will and will not do within the context of the environment explained above. It is where the evaluation is scoped and the cost/benefit of providing assurance of security functions is outlined. It is this section that allows cost-effective evaluations. This cannot be stressed enough. The division of the threats into TOE and environment allows mitigation of risk instead of requiring complete risk avoidance through IT. Therefore, clause 5.1 should be rewritten to reflect this fundamental principle and clause 5.2 should be rewritten to talk about how and why one allocates aspects of threats to TOE and environmental considerations.

43. page 35, clause 6.2.1, paragraph 202: add material cautioning adding SFRs without considering whether they are necessary to meet the objectives at hand. Such padding may sound like a good idea, but it should be remembered that each SFR added means a rise in cost of evaluation. The SFRs should be sufficient but not excessive.

44. page 35, clause 6.2.2, paragraph 204: this material is redundant with the material in 6.1. This redundancy should be minimized by bringing all material on operations together in one place.

45. Page 35, clause 6.2.2, paragraph 205: iteration will be used when different operations are used for different portions of the TOE. If the same component (with the same operations) applies to the entire TOE, one instance is adequate. It has nothing to do with different dependencies on the same component. Reword this paragraph to be consistent with the purpose of iteration.

46. Page 36, clause 6.2.2, paragraph 213 (among others): it is too prescriptive to say to italicize the text. To simply say to highlight it in some way is sufficient. Remove 'italicise of otherwise'

47. Page 36, clause 6.2.2, missing paragraph: an important point about incomplete operations in a PP is the ability for a PP writer to allow some leeway for the ST writer while restricting it to a range more prescriptive than the 15408 component. For instance, the PP writer may restrict a selection to two of the five possible choices or make an assignment a selection by limiting the possible choices. This is an important concept to fully explain in this section and should be added. Perhaps, this material should be linked to the current paragraph 214, as the 'explanation' outlined there is very unclear.

48. Page 36-37, clause 6.2.2, paragraph 215: the interpretation on an acceptable refinement should be added here: a refinement is acceptable if meeting the refined requirement also means meeting the unrefined requirement.

49. Page 37, clause 6.2.3, paragraph 222: the material listed here has little to do with technical feasibility and is rather about performing a cost/benefit analysis. The best thing to do is to change 220d and the leading sentence to the list to talk about cost/benefit instead of feasibility as technical feasibility is about whether the state of the art in technology is there to provide the needed functions. In addition, item 222a should be reworded as audit will always impact performance – the question is whether the benefit of gathering the information is worth the impact.

50. Page 38, clause 6.2.4, paragraph 227: this section should use the preferred terminology of the standard and avoid terms like ‘non-administrators.’ It should instead be explaining about the different authorized users defined in the FMT class. Change the second sentence to read ‘ For example, the security objectives for the TOE might be undermined if unauthorized users can modify such data.’

51. Page 38, clause 6.2.4, paragraph 227, last sentence: this sentence is complex ansd awkward. Reword as follows ‘ Therefore, FMT components are often included as supporting SFRs.’

52. Page 39, clause 6.2.5, paragraph 230: this paragraph encourages using extended components while it should do just the opposite. As a general rule, the PP/ST author should consider carefully whether a component (or set of components) can be used to reflect the security needs. Often a simple refinement of a component can provide the needed function or assurance sought. However, they need to consider the general rule for an acceptable refinement (above – meeting a refined requirement means that meet the unrefined one). If this is not possible, then extended components should be considered, realizing that the evaluation will require more work.

53. Page 39, clause 6.2.5, paragraph 233b: change ‘administrator’ to ‘user’

54. Page 39, clause 6.2.5, paragraph 233: add an item that says that the statement must be evaluatable – a verdict can be reached or it is possible to know when the requirement is met.

55. Page 40, clause 6.2.5, paragraph 236 and clause 6.2.6, paragraphs 238 and 239: short names should not conflict but similar naming should be provided. The naming convention should make it clear that it is an extended requirement. However, there is nothing wrong with saying that it would belong in the current 15408 hierarchy. For instance, if it is a new vulnerability analysis component that would be between the current VLA.1 and VLA.2 there is no reason not to denote it as such. An example such as this might be to name it AVA_VLA.1a_E to say it is hierarchical to VLA.1 but an extension. Another possibility is to prepend “E_” to it to denote an extended requirement. What ever it is used, the component should be presented in the same format as the standard, and it must be clear which requirements are extended.

56. page 40-41, clause 6.3.1: this clause ignores the fundamental principle that the assurance measures chosen must be linked to the objectives of the TOE. It should clearly state both why the measures (EAL or not) are adequate for the objectives being attempted but not excessive. In particular, paragraph 246 seems to imply that if it doesn’t look like you want to do the work necessary, just decide not to. This is inappropriate. If the objectives are to protect the assets to the nth degree, saying that the n-2 degree is all we can do is not acceptable. Either the objectives need to change or ways to achieve the nth degree must be found. This is the wrong place to decide it isn’t worth doing something – that is determined in the risk analysis (cost/benefit) at the objectives level.

57. page 41, clause 6.3.1, paragraph 247: the selection of an EAL must be justified to be in accordance with the TOE objectives. This paragraph implies that picking an EAL means no further work is required.

58. Page 41, clause 6.3.1, missing material: Add material discussing the extra work of building an assurance package that is not an EAL. This section too strongly assumes an EAL.

59. Page 42, 6.3.2, paragraph 251: Iteration of assurance requirements will be used when a component is refined differently for different portions of the TOE. It has little to do with composed TOEs, although composed TOEs are more likely to have different refinements. Change this paragraph to reflect this distinction.

60. Page 43, clause 6.4.1, paragraph 259, third sentence: the evaluation will be measured against the requirements, NOT against the functions. The important thing is that the functions provided meet the requirements stated. This is the main goal of evaluation and should be reflected here.

61. Page 44, clause 6.5.1: The meaning of ‘requirement’ needs to be clarified, especially in this section. A requirement is something that is verified, and yet requirements on the environment are expressly not

‘evalauted’ in the scheme of the standard. It should be made very clear the differences between assumptions on the environment and requirements for the environment, and when to use each.

62. Page 48, clause 7.1, paragraph 284: these paragraphs should add that the functions are compared to the requirements. It would therefore be best to organize the TSS material so the evaluator can clearly see how the proposed functions meet the requirements.

63. Page 48, clause 7.2, paragraph 286: Remove second sentence. Only a small portion of the evaluation is centered on the TSS. A larger portion is about making sure that the requirements are met and that the objectives are met.

64. Page 49, clause 7.4, paragraph 293. The second sentence is more the norm than the exception. The TSS shows how the developer plans to meet the assurance requirements. Therefore the list of evidence will be central to the assurance portion of the TSS, at all levels.

65. Page 52, clause 8.2, paragraph 302 (among others): the requirement to use tables is unnecessary and inappropriate. Instead, the material should concentrate on what sufficient and necessary means. The references to 302 do not deal with whether an objective is necessary, only that it is sufficient. Just because an objective is linked to a threat doesn’t mean it is necessary – that threat might already by fully covered by another objective. The author should be cautioned against adding too much as it increases cost of evaluation. This also applies to the requirements material in paragraph 309.

66. Page 52, clause 8.2, paragraph 306, first sentence: ‘should not’ is too restrictive – it is fully acceptable for the objectives to include the results of risk analysis, and especially cost/benefit analysis. Soften this by changing it to ‘need not’

67. Page 53, clause 8.3.2, paragraph 313: this implies that only EALs will be in a PP/ST. Change ‘target evaluation assurance level’ to ‘ set of assurance components.

68. Page 54, clause 8.3.2, paragraph 313a: add ‘sufficiently low’ to the list.. It is important that the assurance measures chosen are not overkill for the objectives at hand. In other words, they need to justify why the measures are necessary, not just that they are enough.

69. Page 55, clause 8.3.4, paragraph 319: this material is much too prescriptive. A table is neither necessary nor particularly preferred. A tree diagram works just as well. There is also no need to have multiple rows for multiple occurrences because if the dependencies are satisfied for one occurrence, it is for all. This is mostly a waste of resources. The only thing that is necessary is the last phrase of item 319e – an explanation of any unfulfilled dependencies. Rewrite this entire section to be less about the ‘table’ and more about the analysis that occurs.

70. Page 56, clause 8.3.2, paragraph 325: Make the last paragraph an example, change ‘this might involve showing that’ to ‘ For example,’

71. Page 56, clause 8.3.2, paragraph 326b: this is an untrue statement. The FPT class supports assurance directly. The FMT class supports assurance by defining security attributes and management that is reflected in the administrator guidance. This should be reworded.

72. Page 56, clause 8.3.2, paragraph 329: the instance of ‘prevent’ are too strong. These contribute to countering these threats but cannot prevent them.

73. Page 60, clause 9.3.6, paragraph 346: both a and b refer to PP items being ‘met’ or ‘satisfied’. This is not done in a PP compliance claim. The determination of satisfaction is done in the course of the TOE evaluation. This is a simple inclusion of the same material. Soften these terms.

74. Page 60, clause 9.3.6, paragraph 347: change ‘complicated’ to ‘meaningful’.

75. Page 61, clause 9.3.8, paragraph 352: the word ‘dependencies’ is problematic. If this is 15408 dependencies, then it would be reflected in the requirements above. If it is another type of dependency, this needs to be explained.

76. Page 62, clause 10.1, paragraph 355: A composite TOE might also contain PPs but have some components that are in this PP/ST only – in other words build on other PPs. This is actually more likely to be the norm.

77. Page 62, clause 10.1, paragraph 358: The first sentence is awkward. Change to ‘It should be noted that, to date, there has been little practical experience in the area of composability.’

78. Page 63, clause 10.2.4, paragraph 368: The first sentence is confusing. If there is a uniform level of assurance for the entire composite TOE, the statement is just made once, and has nothing to do with having an EAL. Clarify the text.

79. Page 64, clause 10.2.4, paragraph 369: clarify by adding 'the high assurance of' before 'SFR's' in the last sentence.

80. Page 64, clause 10.2.4, paragraph 371: delete this paragraph as it makes no sense. If the objectives require high assurance, then it is necessary. In addition, dependencies between assurance components mean it will be hard to just use a few.

81. Page 64, clause 10.2.5, paragraph 373: The TSS for a composite TOE will almost always need to be rethought as the whole is not merely the combination of the parts. The author will need to consider how the combination of functions now meets the combination of requirements, especially how the different functions contribute and support one another.

82. page 65, clause 10.2.6, paragraph 375c: one area of dependencies different for composed TOEs is that some of the component TOEs may have dependencies that were argued away that no longer need to be – they were on the the environment and now the combination brings the environment into the TOE itself. This should be discussed here.

83. Page 65, clause 10.2.6, paragraph 375d: the use of 'component' is confusing because that term is reserved in 15408. After a second reading, it was clear that it referred to system components. This should be made clear.;

84. Page 65, clause 10.3.1, paragraph 377: The point of a component TOE is that it will be placed in bigger products and systems. The exact combination is generally not known in the context of the component TOE evaluation. Therefore, this section should talk about describing, in generic, terms the types of composed TOEs that might use this component. In fact, any TOE can be used in a bigger composed TOE, and this should be explained in this section of the guidance.

85. Page 65, clause 10.3.2, paragraph 378: The first sentence is false and misleading. The environment sets the context for the evaluation of the component TOE. For small component TOE's this will likely be very generic statements of the types of environments in which to place the TOE. It will likely emphasize the IT environment and assumptions on which it relies. This section should talk about the important roles of assumptions in this type of TOE.

86. Page 66, clause 10.3.3, paragraph 380: This paragraph is internally inconsistent. If there are dependencies on the environment, then the SFRs will not address them. Clarify the meaning of this paragraph.

87. Page 66, clause 10.3.3, paragraph 381: It is generally not allowed to allow one conforming TOE to meet an objective in the environment while another meets it in the IT as the TOE's are no longer comparable. It is important that the PP say what must be in the TOE.

88. Page 66, clause 10.3.4, paragraph 383: Point out that the requirement here could be that a different PP is met (an O/S that meets the xxx PP)

89. page 66, clause 10.3.5, paragraph 384: the component TOE has no knowledge of the composite TOE. The TSS is about this TOE, not about other TOEs. It needs to be clear that the reason for evaluating a component TOE is in order to keep the scope small.

90. Page 66, clause 10.3.5, paragraph 386: The TSS is a specification of the TOE, not the environment. Remove this paragraph.

91. page 68, clause 11.1: This section misses the central point that a package is a portion of a PP/ST that can be reused. All the PP sections for that portion should be completed, to the extent possible. The rest is left as TBD or even as environmental assumptions. It may also be a complete set of either functions or assurances that can be applied to packages of the other type (such as EALs).

92. Page 68, clause 11.1, paragraph 390: The term 'obvious' is inappropriate. The benefits should be listed.

93. Page 68, clause 11.1, paragraph 391: although 15408 doesn't have requirements for packages, the APE/ASE requirements can be extrapolated to apply to the portion being written.